



DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
1509 OLD IRONSIDES AVENUE
FORT KNOX, KENTUCKY 40121-5165

REPLY TO
ATTENTION OF:

ATZK-IO

27 August 2009

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Thunderbolt Policy Memo No. 44-12 – Portable Electronic Devices (PEDs) and Removable Storage Media Travel Security

1. References.

- a. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- b. AR 735-5, Policies and Procedures for Property Accountability, 28 February 2005.
- c. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.
- d. Army Best Business Practice 03-EC-M-0003, Wireless Security Standards, Version 1.26, 22 June 2004, updated 11 August 2006.
- e. VCSA ALARACT 147/2007, 110029ZJUN 07, subject: Safeguarding and Reporting Procedures for Personally Identifiable Information (PII).
- f. AR 25-2, Information Assurance, 24 October 2007.
- g. Memo, HQ USAARMC, IMSE-KNX-IMA, 5 November 2007, subject: Fort Knox Policy Memo No. 22-07 – Personally Identifiable Information (PII).

2. Purpose. The purpose of this policy is to create and disseminate information concerning PEDs and removable storage media travel security.

3. Applicability. This policy applies to all Armor Center Soldiers, civilians, and contractors who take Government-assigned PEDs/media from the Government workplace.

4. Policy.

- a. Failure to adequately protect PEDs and removable storage media continues to be a leading factor in the loss of PII and For Official Use Only (FOUO) Army data. These losses reduce effectiveness of the command and places our mission in jeopardy. All activities will ensure all PEDs and removable storage media containing PII/FOUO data are protected.

ATZK-IO

SUBJECT: Thunderbolt Policy Memo No. 44-12 – Portable Electronic Devices (PEDs) and Removable Storage Media Travel Security

b. All users of PEDs and removable storage media will ensure their devices have an encrypted folder for storage of PII/FOUO data and are properly labeled with FK Form 5078 (for laptops) or FK 5078a (for thumb drives). The PEDs and removable storage media, by default, should NOT contain PII/FOUO information. The PII/FOUO information should only be stored by exception and when mission accomplishment necessitates its usage. If this information is stored on PEDs and removable storage media, it will be encrypted. Once PII/FOUO information is no longer needed, it should be deleted from the device(s) or media. All users will be trained in the protection of PII/FOUO data and use of Department of the Army-approved encryption software and receive annual refresher training.

c. The PEDs include laptops, Blackberries, and similar devices, and removable storage media includes items such as CDs, DVDs, floppy disks, thumb drives, flash memory, memory sticks, magnetic tape, other optical media, external or removable hard drives, and other similar PEDs/mobile media devices. Any item that contains PII/FOUO (e.g., Privacy Act, HIPPA, Proprietary data) is subject to this policy. Violation of paragraphs 4d through g of this policy is punitive. Military personnel violating this policy may be subject to action under the Uniform Code of Military Justice and/or adverse administrative action. Civilian employees who violate this policy may also be subject to adverse or disciplinary action in accordance with applicable laws and regulations.

d. Ensure PEDs and removable storage media used for travel are identified and labeled to indicate they are authorized for travel. When traveling with PEDs or removable storage media devices to any place outside the Government workplace (i.e., hotel, home, meeting site, etc.), the device or media must have all PII/FOUO information in an encrypted form. The traveler must carry the device/media with him/her (whenever feasible) or always maintain positive physical and visual control of the device/media. When leaving an area and carrying the device/media is not practical, it must be locked in a reasonably secure container or placed under the control of a co-worker. For laptops, cable and lock mechanisms shall be used to secure the computer to a difficult-to-move object if the device may be exposed to theft.

e. While traveling by airplane, train, or bus, devices must NOT be checked with other baggage. The preferred method of security is the traveler hand carrying the device and carefully storing and retrieving the device from the overhead bin or under the seat. The device must remain within the traveler's sight and within immediate reach at all times.

f. While traveling by private- or Government-owned vehicle, PEDs or removable storage media devices must not be left in vehicles that do not have a contained trunk. Laptop users must use an approved cable and lock for added security when using the trunk of a vehicle for short-term storage. The preferred method of security is the traveler hand carrying the device and keeping it within sight and immediate reach at all times.

ATZK-IO

SUBJECT: Thunderbolt Policy Memo No. 44-12 – Portable Electronic Devices (PEDs) and Removable Storage Media Travel Security

g. No PEDs or removable storage media devices containing PII/FOUO information will be used for travel or removed from a defense installation or Government-controlled facility unless the following criteria are met:

(1) An Army-approved encryption solution is loaded and active, and PII/FOUO data is encrypted on the device.

(2) Required labels are affixed to the outside cover of the laptop and to smaller portable devices, such as the Blackberry, thumb drives, and other portable media, so they will be visible for inspection. The labels will state they comply with the Army data encryption standard and are authorized for travel. The labels are available and can be downloaded from the Fort Knox E-forms website at <http://www.knox.army.mil/garrison/doim/forms/fkforms.html>.

h. Neither PEDs nor removable storage media devices will be left unattended and unsecured in the workplace. While in the office and the device is not under one's immediate control, lock the device in the office, secure it with a locking cable mechanism, or place the device in an appropriate container (such as a safe, lockable closet, or lockable cabinet).

i. All computer devices shall be hand receipted. The PEDs and media approved for travel will be hand receipted as personal issue equipment. Liability for loss or theft of computer devices shall be evaluated in accordance with this policy and AR 735-5. Failure to follow this policy or other guidance on laptop security may constitute negligence and subject the violator to personal financial liability.

j. Laptops are prohibited from use in classified or sensitive areas, including offices that have Secret internet protocol router network (SIPRNET) connections or equipment, unless specifically accredited for SIPRNET use.

k. In the event a device or media containing PII/FOUO data is lost, stolen, or destroyed, the user will immediately notify his/her director/commander. The director/commander will:

(1) Immediately notify the Fort Knox Installation Operations Center at (502)-624-5151.

(2) Notify the US-CERT at <http://www.us-cert.gov> **within 1 hour** of discovering the incident.

(3) Immediately send an e-mail to piireporting@us.army.mil including information obtained on FK Form 5080-E and provide a copy of the e-mail to the Knox Information Assurance Office at KnoxIAOffice@conus.army.mil.

ATZK-IO

SUBJECT: Thunderbolt Policy Memo No. 44-12 – Portable Electronic Devices (PEDs) and Removable Storage Media Travel Security

(4) Complete a serious incident report detailing the data involved and circumstances of the loss.

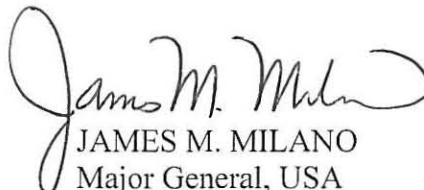
(5) Coordinate with the local Staff Judge Advocate for sending affected individuals the notification letter within 10 days.

l. The PEDs containing or used with PII/FOUO data shall use the Common Access Card as the primary means of authentication. Blackberry devices will be configured to require the use of a password for access.

m. Personal (non-Government owned) devices and media will NOT be used to store or transport Government proprietary or PII/FOUO data.

n. In addition to the mandatory procedures above, commanders and supervisors will be vigilant and proactive. Physical security is the first line of defense. Commanders and supervisors must evaluate the risk and vulnerabilities of loss and theft and take all reasonable measures necessary for ensuring adequate safeguards are in place for all Government-owned/leased PEDs and removable storage media containing PII/FOUO data.

o. Although portions of this policy are punitive, commanders and supervisors are reminded to consider the full range of options for addressing misconduct and disposing the case at the lowest appropriate level consistent with the gravity of the misconduct.


JAMES M. MILANO
Major General, USA
Commanding

DISTRIBUTION:

C plus

1 - Each Activity IMO and IASO